Background

If an executable file is found on a share and is writable to other users it is possible for those users to alter the executable, and wait for a legitimate user to execute the file, and thereby gain remote code execution. This is not something that we might want to do on assessments, but good attack vector for a real attacker.

How to test for

See the Tools chapter for how to install PowerSploit.

The best way to find executables where your domain user has write-access is by using the PowerSploit cmdlet `find-interestingFile`. It will correcly show that if the user has writable access even if it is by belonging to a group.

```
Find-InterestingFile -Path A:\ -CheckWriteAccess -Include @('*.exe') | export-csv result.csv
```

References

https://www.harmj0y.net/blog/redteaming/targeted-trojanation/